CMSC 39600 – Lec #15 (Nov 15)

Today

- PCP Theorem (another proof)

PSet 2 – submit electronically

Extra lecture – TTI ; No lecture – Nov 20

Guest lecture – J. Chuzhoy (Nov 27)

Toolkit

1. **Low-Degree Test**

$\exists \epsilon_0 = \min\left(\frac{d}{q}\right)^{\beta}$ $\forall \epsilon$

$$\delta(f, P_d^m) > \epsilon \Rightarrow \Pr_{\substack{\rho\text{-plane} \\ x \notin \rho}} [f(\rho)(x) \neq f(x)] > \epsilon - \epsilon_0$$

---

2. **Schwartz-Zippel:**

$p, q : \mathbb{F}^m \to \mathbb{F}$ – 2 distinct d m-variate deg d poly

$$\Pr_x [p(x) \neq q(x)] \geq 1 - \frac{d}{q}$$

---

3. **Composition Theorem**

4. CKTVAL $\in$ prob-PCPP$_{1,1-\epsilon_1}[r_1, q_1, d, \text{robust } \rho_1]$ & CKTVAL $\in$ PCPP$_{1,1-\epsilon_2}[r_2, q_2, \delta]$ & $\delta_2(d_1) \leq \rho_1(n)$, then

CKTVAL $\in$ PCP$_{1,1-\epsilon\epsilon_2}[r_1(n) + r_2(d_1(n)), q_2(d_1(n))]$

Out-PCPP w/ proximity δ, so is more composed

In-PCPP prob w/ robust ρ_1 so is composed.

---

4. CKTVAL $\in$ PCPP$_{1-\delta}[O(n^2), 17, 35]$ for all $\delta < \delta_0$.

Game Plan

Begin by proving

$$\text{CKT-SAT} \in \text{PCP}_{1,1/8}[O(\log n), \text{poly}\log n]$$

Massage proof to show

$$\forall \delta \in (0,1), \quad \text{CKT-VAL} \in \text{prob-PCPP}_{1,1-\Omega(\delta)}[O(\log n), \text{poly}\log n, \text{prox} = \delta, \text{robustness} = \Omega(1), \text{decision complexity} = \text{poly}\log n]$$

Composing w/ itself

$$\forall \delta \in (0,1) \quad \text{CKT-VAL} \in \text{prob-PCPP}_{1,1-\Omega(\delta)}[O(\log n) + \log\log n, \text{poly}\log\log n, \text{prox} = \delta, \text{prob} = \Omega(1), \text{decision} = \text{poly}\log\log n]$$

Composing w/ exponential sized PCPP

$$\forall \delta \in (0,1) \quad \text{CKT-VAL} \in \text{PCPP}_{1,1-\Omega(\delta)}[O(\log n) + \text{poly}\log\log n, 17, \text{prox} = \delta]$$

Hence,

$$\text{CKTSAT} \in \text{PCP}_{1,1-\delta}[O(\log n), 17]$$

Arithmetizing the Circuit

C - circuit with n gates (all binary or unary)
& k up gates

$\mathbb{F}$ - field (size q) $\quad H \subseteq \mathbb{F}$ (size h) $\quad q = h\,\text{poly}(m)$

Assignment to gates

$A : [n] \to \{0,1\}$.

$H^m \longleftrightarrow [n] \qquad (h^m = n)$

$A : H^m \to \{0,1\}$

Interpolate A to get poly $a : \mathbb{F}^m \to \mathbb{F}$

s.t. $a|_{H^m} \equiv A$

$\forall i$ $\deg_{x_i}(a) \le |H| = h$, Hence $\deg(a) \le mh$

$A : \mathbb{F}^m \to \mathbb{F}$ (view as assignment by looking at $A|_{H^m}$ (0,1 + others - "don't care")

Circuit C

$C : [n]^3 \times H \to \{0,1\}$ $\qquad C : H^{3m+3} \to \{0,1\}$

$C(i_1, i_2, i_3, b_1, b_2, b_3) = \begin{cases} 1 & \text{if } \omega_{i_1}, \omega_{i_2}, \omega_{i_3} \text{ and } (b_1, b_2, b_3) \in \{0,1\} \\ & \text{and } (\omega_{i_1} = b_1) \wedge (\omega_{i_2} = b_2) \wedge (\omega_{i_3} = b_3) \\ 0 & \text{otherwise.} \end{cases}$

Interpolate C to get $\hat{C} : \mathbb{F}^{3m+3} \to \mathbb{F}$

deg in each variable $\le h$, tot deg $\le (3m+3)h$.

$A : \mathbb{F}^m \to \mathbb{F} \overset{p^C}{\rightsquigarrow} p^C_{(A)} : \mathbb{F}^{3m+3} \to \mathbb{F}$

$p^C_{(A)}(u,v,w,a,b,c) = \hat{C}(u,v,w,a,b,c)(A(u)-a)(A(v)-b)(A(w)-c)$

Observe: $p^C_{(A)}|_{H^{3m+3}} \equiv 0 \iff A|_{H^m}$ is a satisfying assignment

Reduction R

$\{\text{Circuit } C\} \longmapsto \{\text{Mapping } P^C\}$

$P^C : \{A : \mathbb{F}^m \to \mathbb{F}\} \longmapsto \{P : \mathbb{F}^{3m+3} \to \mathbb{F}\}$.

If $\deg(A) \le mh \Rightarrow \deg\left(P^C_{(A)}\right) \le (6m+3)h = d$

Choose q s.t $\epsilon_0 = m^d\left(\frac{d}{q}\right)^B$ is small

ie, $q = \not{d} \cdot \text{poly}(m) = h \cdot \text{poly}(m)$. / h^2

Recall If $q^m = \text{poly}(n)$, reduction is poly time

$m^m = \text{poly}(n)$

Choosing $m = \frac{\log n}{\log\log n}$, $m^m = \text{poly}(n)$. / $h = \text{poly}\log n$, $q = \text{poly}\log n$

(1) If C is satisfiable, there exist poly $a : \mathbb{F}^m \to \mathbb{F}$ of $\deg \le mh$ such that $P^C_{(a)} : \mathbb{F}^{3m+3} \to \mathbb{F}$ satisfies $P^C_{(a)}\big|_{H^{3m+3}} \equiv 0$

(2) If C is not satisfiable, then $\forall$ functions $A : \mathbb{F}^m \to \mathbb{F}$, $P^C_{(A)}\big|_{H^{3m+3}} \not\equiv 0$

Furthermore P_C maps deg mh poly to $(6m+3)h$ deg poly.

~~$h = \text{poly}\log m$~~

How to check $P|_{H^m} \equiv 0$?

Define $Z_H(x) = \prod_{h \in H} (x - h)$ (univariate poly)

ie, $x \in h \iff Z_H(x) = 0$

Claim: $P|_{H^m} \equiv 0$ (P deg d) iff there exist m deg d poly$_m$ $P_1 \ldots P_m$

$$p(x_1 \ldots x_m) \equiv \sum_{i=1}^{m} Z_H(x_i) \cdot P_i(x_1 \ldots x_m)$$

Hence proof that $P|_{H^m} \equiv 0$ is the list of poly $P_1 \ldots P_m$.

Bundling: $C_1, C_2 \subseteq \Sigma^n$ (2 codes)

$C_1 \odot C_2 \subseteq (\Sigma^2)^n$ $\quad C_1 \odot C_2 = \{(z_1^{(1)}, z_1^{(2)}), (z_2^{(1)}, z_2^{(2)}), \ldots (z_n^{(1)}, z_n^{(2)}) \mid (z_1^{(1)}, \ldots z_n^{(1)}) \in C_1\}$.

Claim: $\forall z \in (\Sigma^2)^n$, $\delta(z|_{(1)}, C_1) > \delta \Rightarrow \delta(z, C_1 \odot C_2) \geq \delta$.

Code - Reed Muller m-variate deg d poly $P_{m,d}$

$p \in \mathbb{F}^{q^m}$ $\quad (p(x_1), \ldots, p(x_{q^m}))$

m-Bundled Reed Mullex $P_{m,d}^{\odot m}$

$P_1, P_2, \ldots P_m : \mathbb{F}^m \to \mathbb{F}$

$p : \mathbb{F}^m \to \mathbb{F}^m$ s.t $p(x_1 \ldots x_m) = (P_1(x), \ldots, P_m(x))$

Cor: For any $Q : \mathbb{F}^m \to \mathbb{F}^m$, $\delta(Q, P_{m,d}^{\odot m}) \leq \delta \Rightarrow \forall i \; \delta(Q_i, P_{m,d}^{\odot m}) \leq \delta$.

Given circuit C, want to check if

$\exists$ deg m poly $a: \mathbb{F}^m \to \mathbb{F}$ s.t $P^C_{(a)}|_{H^{3m+3}} = 0$.

Expect as proofs:

$A: \mathbb{F}^m \to \mathbb{F}$ (a

$P_0: \mathbb{F}^{3m+3} \to \mathbb{F}$ ($P^C_{(a)}$

$P: \mathbb{F}^{3m+3} \to \mathbb{F}^{3m+3}$ ($P = (P_1, \ldots P_m)$ s.t $P_0 = \sum_{H} z_H P_i$)

& also plane oracles for $A, P^1, \ldots P^m$

PCP Verifier

1. Choose random plane $\rho \in \mathbb{F}^m$ & $x \in \rho$
   check if $A(\rho)(x) = A(a)$
2. Choose random plane $\rho \in \mathbb{F}^{3m+3}$ & $x \in \rho$
   check if $\forall i$, $P_i(\rho)(x) = P_i(x)$
3. Choose a random point
   $z = (v, r, \omega, a, b, c) \in \mathbb{F}^{3m+3}$
   check if
   $\hat{C}(v, r, \omega, a, b, c)\,(A(v)-a)(A(r)-b)(A(\omega)-c) = \sum_H z_H(z_i) P^i(z)$

Randomness $= 3(3m+3)\log|\mathbb{F}| + 3m \log \mathbb{F} + (3m+3)\log|\mathbb{F}|$

$= O(\log n)$

Query Complexity $= (3m+3)\,|\mathbb{F}|^2 \log|\mathbb{F}|$

$= \text{poly} \log n$

Bundled LDT

$\delta(f, P_{m,d}^{\oplus n}) \geq \delta \Rightarrow Pr[rej] \geq \delta - \epsilon_0$

Suppose C is not satisfiable (ie, $\nexists a$ s.t. $P_{(a)}^{c}|_{H^{3m+3}} \equiv 0$)

For any ϵ s.t. $\frac{d}{q} + 5\epsilon \leq 1 + \epsilon_0$.

Case(i) $\delta(A, P_{m,d}) \geq \epsilon \Rightarrow Pr[rej] \geq \epsilon - \epsilon_0$

Case(ii) $\delta(P, P_{3m+3,d}^{\oplus(3m+3)}) \geq \epsilon \Rightarrow Pr[rej] \geq \epsilon - \epsilon_0$.

Case(iii) $\exists$ poly $a \in P_{m,d}$ & polys $P_1 \ldots P_{3m+3} \in P_{3m+3,d}$ s.t.
$\delta(A, a) \leq \epsilon$ & $\delta(P, P_1 \oplus P_2 \oplus \ldots \oplus P_{3m+3}) \leq \epsilon$

It is not true that

$\hat{C}(a) = \sum z_H P_i$

Hence $Prob[rej] \geq 1 - \frac{d}{q} - 3\epsilon - \epsilon = 1 - \frac{d}{q} - 4\epsilon \geq \epsilon - \epsilon_0$.

$Pr[rej] \geq \epsilon - \epsilon_0$.

Claim: If A is ϵ-far from any deg d poly m s.t. $a|_{H^{3m}}$ is a sat assignment, then
$Pr[rej] \geq \epsilon - \epsilon_0$.